UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MINNESOTA

ARTHRITIS AND RHEUMATOLOGY ASSOCIATES OF SOUTH JERSEY, P.C., Individually and on behalf of all others similarly situated, Plaintiffs, v. UNITEDHEALTH GROUP, INCORPORATED, and CHANGE HEALTHCARE, INC., and UNITEDHEALTHCARE, INC., and OPTUM, INC., Defendants.	Case No. 24-cv-02443 CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

COMPLAINT

Plaintiff Arthritis and Rheumatology Associates of South Jersey, P.C. ("Arthritis and Rheumatology Associates") individually and on behalf of all others similarly situated, complaining of Defendants Change Healthcare, Inc. ("Change"), UnitedHealth Group, Incorporated ("UHG"), UnitedHealthcare, Inc. ("UnitedHealthcare"), and Optum, Inc. ("Optum"), hereby avers as follows:

NATURE OF THE ACTION

1. Defendant Change is a healthcare technology company that is owned by Defendants UHG and Optum. Change operates a software platform that connects medical practices with payers, pharmacies, and patients in order to streamline the process by which medical practices manage patient visits, collect revenue, and access patient information.

2. This class action complaint arises from a massive data breach that began on February 12, 2024, when Blackcat, a group of cybercriminals, accessed Change's networks, exfiltrated and encrypted the personal information and healthcare records of millions of individuals and medical practices, and held the stolen information for ransom (the "Data Breach"). As is set forth in more detail below, the Data Breach was foreseeable and could have been prevented through the implementation of industry-standard cyber security measures and protocols.

3. As a result of the Data Breach, Defendants took the Change platform offline and left medical practices such as Plaintiff without the ability to find and verify patient information, manage their billing cycles, and submit bills to insurance companies. The inability to perform basic administrative and billing tasks has caused substantial losses for Plaintiff and other medical practices, including but not limited to uncollected revenue, loss of income from procedures that could not be pre-certified, and loss of patients.

PARTIES

4. Plaintiff Arthritis and Rheumatology Associates is a New Jersey professional corporation with a principal place of business located at 2848 South Delsea Drive, Vineland, NJ 08360. 1100 Liberty Place, Sicklerville, NJ 08081. Arthritis and Rheumatology Associates utilized the Change platform prior to the Data Breach and sustained significant financial injuries as a result of the Data Breach.

5. Defendant UHG is a Delaware corporation with a principal place of business located at UnitedHealth Group Center, 9900 Bren Road East, Minnetonka, MN. UHG is one of the largest health insurers in the United States and is the parent corporation of Defendants UnitedHealthcare and Optum.

6. Defendant Change is a Delaware corporation with a principal place of business located at 24 Church Street #1400, Nashville, TN. Despite hosting a platform that stored confidential medical and financial information for millions of patients, Change failed to adopt industry-standard cyber security measures and protocols, thereby enabling the Data Breach. Change is a subsidiary of Defendant Optum, which is itself a subsidiary of Defendant UnitedHealth.

7. Defendant UnitedHealthcare is a Delaware corporation with a principal place of business located at UnitedHealth Group Center, 9900 Bren Road East, Minnetonka, MN. UnitedHealthcare markets and sells health insurance policies and related services privately and through the Affordable Care Act marketplace. UnitedHealthcare is a subsidiary of Defendant UHGroup.

8. Defendant Optum is a Delaware corporation with a principal place of business located at 13625 Technology Drive, Eden Prairie, MN, 55344. Optum provides health technology products and services intended to increase efficiency in the healthcare industry through data and analytics. Optum is the parent corporation of Change and a subsidiary of UHG.

JURISDICTION AND VENUE

9. This Court has jurisdiction over this matter pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d)(2) because the amount in controversy exceeds $5 million, there are more than 100 putative members in the proposed class, and Plaintiff is a citizen of a state different from any Defendant. This Court has supplemental jurisdiction over state law claims arising from the same case or controversy pursuant to 28 U.S.C. §1367.

10. Defendants are subject to the jurisdiction of this Court because each Defendant regularly and intentionally conducts business within the State of Minnesota.

11. Venue is proper in Minnesota because Defendants UHG, UnitedHealthcare, and Optum have principal places of business in Minnesota.

OPERATIVE FACTS

The Data Breach

12. Change is a healthcare technology clearinghouse that provided a suite of crucial services to Plaintiff and other medical practices until UHG severed connectivity with Change's data centers on February 21, 2024 after learning of the Data Breach and ransom demand.

13. Change stores massive amounts of data relating to patient care, insurance coverage, billing, and prescriptions that medical practices used to verify patient insurance, obtain pre-certifications prior to performing procedures, input billing codes, process prescription orders and payments, and generally manage payment cycles.

14. By connecting patients, providers, payers, and pharmacies, Change enables medical practices to streamline and expedite the payment cycle from start to finish. For example, by inputting billing codes into software supported by Change, a medical provider could quickly verify that a patient had coverage for a procedure or prescription, determine the necessary co-pay, and then submit a bill to the insurance company for payment.

15. Change plays a central role in the healthcare industry. Its cloud-based network supported up to 15 billion transactions annually and is estimated to touch one in three U.S. patient medical records.[1]

[1] Nicole Sganga & Andres Triay, *Cyberattack on UnitedHealth Still Impacting Prescription Access: "These are threats to life,"* CBS News (Feb. 29, 2024, 9:00 PM), https://www.cbsnews.com/news/unitedhealth-cyberattack-change-healthcare-prescription-access-still-impacted/.

16. On February 21, 2024, UHG filed a report with the Securities Exchange Commission indicating that a cyber security threat actor had gained access to Change's networks.

17. On or about February 28, 2024, in a post published on its darkweb site, Blackcat claimed responsibility for the attack and claimed to have stolen eight terabytes of data from Change, including patient health data and insurance information.

18. After accessing Change's network, Blackcat installed ransomware, a type of software that encrypts documents and information so that the owner cannot access or use it until a sum of money is paid.

19. In the ordinary course of business, Change collects valuable and confidential patient information such as (1) personal identifiers, (2) payment information, (3) commercial information, (4) visual information, (5) professional and employment information, (6) consumer profiles, preferences, and characteristics, (7) browser and device data, (8) usage data, (9) site activity, and (10) social media accounts and content.[2]

20. The data that Blackcat stole and held for ransom was crucial to Plaintiff's operations and operations of the other healthcare practices that utilized the Change network and data centers.

21. On or about February 22, 2024, Defendant UHG filed a Form 8-K with the Securities Exchange Commission (SEC) acknowledging that a "cyber security threat actor" had

[2] https://www.changehealthcare.com/privacy-notice#:~:text=We%20collect%20your%20name%2C%20phone,the%20Site%20and%20the%20Services (last visited May 21, 2024).

accessed the Change networks and asserting that UHG had "proactively isolated the impacted systems" in order to contain and remediate any damage.[3]

22. On or about March 1, 2024, it is believed that Change paid Blackcat approximately $22 million worth of bitcoin in order to regain access to encrypted data and to prevent stolen information from being published or sold.[4]

23. Despite the ransom payment, Change did not get its data back and Plaintiff and other medical practices continue to suffer significant financial and operational problems as a result of the Data Breach. The danger that the stolen data will be published, sold, and misused by cybercriminals remains.[5]

Effect of the Data Breach on Plaintiff

24. Prior to the Data Breach, Plaintiff utilized Aprima, a practice management and billing software application published by CompuGroup Medical ("CGM"). Specifically, Plaintiff utilized Aprima for tasks including creating patient records, accessing patient records, and filling prescriptions, as well as practice management functions such as scheduling, billing, submitting claims, and verifying patient insurance.

25. Aprima is supported by the Change network's data centers and payment clearinghouse. In other words, Plaintiff enters information and submits claims and inquiries through the software and the software interacts with the Change network to provide information and services.

---

[3] https://www.sec.gov/Archives/edgar/data/731766/000073176624000045/unh-20240221.htm (last visited May 21, 2024).

[4] Andy Greenberg, *Change Healthcare Finally Admits it Paid Ransomware Hackers $22 Million – and Still Faces a Patient Data Leak*, Wired (April 22, 2024, 11:55 PM) https://www.wired.com/story/change-healthcare-admits-it-paid-ransomware-hackers/ (last visited May 22, 2024).

[5] Id.

26. The Change network allows medical practices to access patient records stored in Change data centers through the practices' software. Similarly, when a medical practice enters billing codes into their software, the software connects to the Change clearinghouse which processes the bill and submits it to the applicable payer for remittance.

27. The Change network also streamlined the process of obtaining pre-certifications for prescriptions and procedures. Rather than engage in the cumbersome process of entering patient information and billing codes to each individual patient's insurance company, the Change network centralized this information so that it could be submitted in batches through a single software program.

28. On February 21, 2024, Plaintiff experienced an interruption in its ability to obtain pre-certifications and submit claims through Aprima.

29. On February 22, 2024, Plaintiff received an email from CGM explaining that there had been a "cyber security issue at Change Healthcare/Optum Solutions" and that transactions processed through the Change network would be delayed or unavailable until the issue was resolved.[6]

30. On February 27, 2024, Plaintiff received an email from Aetna, a large health insurer for whom Plaintiff was in-network, explaining that the Change network had been taken offline and suggesting alternate means for obtaining pre-certifications and submitting claims while the Change Electronic Data Interchange was unavailable. Aetna also acknowledged the breadth of the problem, noting that "Aetna uses Change Healthcare as an intermediary for certain Electronic Data Interchange (EDI) transactions across all of our lines of business."[7]

[6] *See* Exhibit A, February 22, 2024 Email.
[7] *See* Exhibit B, February 27, 2024 Email.

31. On February 28, 2024, Plaintiff received an email from Horizon Blue Cross Blue Shield of New Jersey ("Horizon") explaining that their business operations had also been affected by the Data Breach and the disabling of the Change network.[8]

32. Despite the efforts of insurers like Aetna and Horizon to provide alternative portals for obtaining certifications and submitting claims, Plaintiff remained unable to adequately perform these necessary functions because many transactions still required access to the Change network. For example, Plaintiff was often unable to obtain Electronic Remittance Advice (ERA), which is the explanation of a patient's coverage and any adjustments thereto. ERAs are a crucial component of the medical billing cycle.[9]

33. Plaintiff's practice suffered significant losses while the Change platform was offline as a result of its inability to submit electronic claims, receive payments, perform eligibility verifications, and obtain ERAs.

34. Utilizing the alternative portals suggested by insurers like Aetna and Horizon was an inefficient and cumbersome process that required Plaintiff's employees to spend significantly more time on each transaction than they had spent prior to the Data Breach. Moreover, the alternative portals often required payment per transaction instead of a flat periodic fee which increased Plaintiff's operational costs.

35. On April 11, 2024 Aetna sent an email to Plaintiff explaining that they had restored the connection to the Change network. However, Aetna also acknowledged that there was a significant backlog of ERAs that had not been processed since the February 21, 2024 Data Breach.[10]

[8] *See* Exhibit C, February 28, 2024 Email.
[9] *See* Exhibit D, March 6, 2024 Email.
[10] *See* Exhibit E, April 11, 2024 Email.

36. On May 29, 2024, more than three months after the Data Breach, Plaintiff received another notice from Aetna acknowledging that certain electronic claims submitted on or after February 21, 2024 were still not processed or accounted for. Specifically, Aetna explained that Change Healthcare would have no record of claims submitted through Plaintiff's Payer ID for the Government Employees Health Association and that Plaintiff would not have received any rejection notice informing them of the particular claims that were not processed.[11]

37. The unavailability of the Change network caused an interruption in Plaintiff's ability to submit claims for payment and to obtain certifications and ERAs. This loss of functionality resulted in increased costs to Plaintiff and decreased revenue.

Defendants' Failure to Adhere to Industry Cyber Security Standards Enabled the Occurrence of the Preventable Data Breach

38. Because the health insurance industry collects, stores, and uses massive amounts of patient information, the industry is governed by a regulatory and statutory framework designed to protect patients' privacy.

39. Defendants are covered by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), including the Security Standards set forth in 45 C.F.R. §§164.306 – 164.318 and the Privacy Rules set forth in 45 C.F.R. §§164.500 – 164.535 ("HIPAA Privacy Rules").

40. The HIPAA Security Standards required Defendants to:

a. Ensure confidentiality, integrity, and availability of electronic health information that they created, received, or maintained;

[11] *See* Exhibit F, May 29, 2024 Email.

b. Protect against reasonably anticipated threats or hazards to the security or integrity of patient information;

c. Protect against reasonably anticipated uses or disclosures not permitted by HIPAA; and

d. Ensure that their workers complied with HIPAA.

See 45 C.F.R. §164.306.

41. The HIPAA Privacy Rules also required or advised Defendants to:

a. Implement policies and procedures to prevent, detect, contain, and correct security violations including through risk analysis, risk management, sanctions policies, and information system activity reviews;

b. Implement policies and procedures to ensure that members of the workforce who need to access protected health information have access and that those members of the workforce who do not need to access protected health information do not have access;

c. Isolate health care clearinghouse functions so that information held by the clearinghouse is protected from unauthorized access by the larger organization;

d. Implement cyber security awareness training for its workforce;

e. Implement procedures for monitoring log-in attempts and periodically changing and safeguarding passwords;

f. Establish a data backup plan and disaster recovery plan so that exact copies of protected health information can be restored and retrieved in the event of a loss of data; and

g. Establish an emergency mode plan to enable continuation of critical business processes for the protection and use of protected health information during an emergency.

See 45 C.F.R. §164.308.

42. The health insurance and technology industries are also regulated by the Federal Trade Commission ("FTC"), which promulgates rules and best practices for the collection, storage, and protection of data. The FTC also has the power to enforce antitrust and consumer protection laws, including the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, which prohibits unfair or deceptive practices in commerce.

43. The FTC has published guidelines for businesses to follow to protect sensitive data. The FTC guidelines instruct businesses to implement data security practices such as: (1) taking stock of what personal information is being collected, how it is being collected, and from whom it is being collected; (2) scaling down the collection and storage of personal information and keeping only what is necessary; (3) locking stored personal information by identifying all connections to computers that stored personal information and encrypting sensitive information and transmissions; (4) properly and securely disposing of information that is no longer necessary; and (5) creating a plan of action in the event of a breach to ensure that compromised devices and systems are promptly disconnected and that other appropriate investigative and remedial steps are taken without delay.[12]

44. Regarding the safe storage of electronic information, the FTC recommends further that businesses take steps such as: (1) encrypting all sensitive information that is stored or

[12] *Protecting Personal Information*, FTC, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited May 24, 2024).

disseminated to third parties; (2) maintain up-to-date anti-malware programs on all computers and servers; (3) checking websites of the Cybersecurity & Infrastructure Security Agency and software vendors for alerts as to new vulnerabilities and patches; (4) restricting employees' ability to download unauthorized software; (5) scanning computers to identify and close unnecessary network connections; (6) adding additional layers of encryption to particularly sensitive information; and (7) monitoring web applications which can be particularly susceptible to certain kinds of hacks.[13]

45. The FTC also recommends that all business employ certain basic measures to protect their network such as (1) using multi-factor authentication and requiring regular password changes; (2) locking network devices after a period of inactivity; (3) installing firewalls; and (4) encrypting information that is sent over a wireless connection.[14]

46. According to the FTC, a company's failure to maintain reasonable and appropriate data security measures amounts to an unfair trade practice in violation of the FTCA.[15]

47. In addition to the FTC, other agencies and organizations such as the National Institute of Standards and Technology and the Center for Internet Security ("CIST") provide similar publications aimed at helping businesses protect their networks and sensitive information.

48. The various statutes, regulations, and guidelines collectively establish industry standards regarding basic, fundamental cybersecurity best practices. In sum, all businesses in the

[13] Id.
[14] Id.
[15] *Collecting, Using, or Sharing Consumer Health Information? Look to HIPAA, the FTC Act, and the Health Breach Notification Rule*, FTC, https://www.ftc.gov/business-guidance/resources/collecting-using-or-sharing-consumer-health-information-look-hipaa-ftc-act-health-breach (last visited May 24, 2024).

healthcare, health insurance, and health technology industries should (1) restrict access to sensitive information; (2) utilize strong passwords and multi-factor authentication; (3) install firewalls and updated anti-malware programs; (4) monitor traffic to servers and networks; (5) encrypt stored and transmitted data; (6) educating employees on basic cybersecurity principles; and (7) perform regular backups of all stored information and data.

49. Defendants failed to adhere to applicable cybersecurity statutes, regulations, guidelines, and industry standards for the safe storage of sensitive information.

50. Defendants violated HIPAA and the FTCA, and failed to meet industry standards, by:

(a) Failing to maintain an adequate date security system;

(b) Failing to protect patients' sensitive information;

(c) Failing to prevent the theft and possible dissemination of sensitive information;

(d) Failing to implement policies to restrict network and data access to properly authorized individuals;

(e) Failing to address credible security warnings and threats;

(f) Failing to maintain up-to-date security patches to remediate vulnerabilities;

(g) Failing to monitor the CIST website for information about current threats and associated patches;

(h) Failing to utilize adequate encryption for the storage and transmission of sensitive information;

(i) Failing to maintain audit logs and access reports to understand exactly how and by whom their network was being accessed; and,

(j) Failing to train employees on basic cybersecurity principles.

51. In a letter to the Securities and Exchange Commission, Senator Ron Wyden requested an investigation of UHG and its failure to implement adequate and industry standard cybersecurity measures.[16]

52. In his letter, Senator Wyden concluded that "the audit committee of UHG's board, which is responsible for overseeing cybersecurity risk to the company, clearly failed to do its job."[17]

53. Senator Wyden also noted that neither UHG's top cybersecurity official nor the members of UHG's audit committee had meaningful cybersecurity expertise, writing "One likely reason for UHG's negligence, and the company's failure to adopt industry-standard cyber defenses, is that the company's top cybersecurity official appears to be unqualified for the job. Steven Martin, UHG's chief information security officer (CISO), had not worked in a fulltime cybersecurity role before he was elevated to the top cybersecurity position at UHG in June 2023."[18]

54. At all times material hereto, Defendants knew or should have known that the sensitive and confidential personal information stored on the Change platform was an attractive target for cyber criminals.

---

[16] Noah Barsky, *What If The Scathing UnitedHealth Cyber Rebuke Was Yours?*, Forbes (June 5, 2024, 8:00 AM) https://www.forbes.com/sites/noahbarsky/2024/06/05/what-if-the-scathing-unitedhealth-cyber-rebuke-was-yours/ (last visited June 18, 2024)

[17] Id.

[18] Id.

55. Defendants knew or should have known that Cybercriminals frequently target healthcare organizations because of the bulk and unique value of the patient information that is stored on their networks. Indeed, the personal identifiers, financial information, and medical data stored by healthcare organizations can be readily utilized by or sold to identity thieves for large sums of money.

56. Upon information and belief, Defendants were aware of the value of the information they stored as well as their vulnerability to cyber-attacks.

57. Defendants were also aware that a breach of their cyber security systems could have devastating effects on patients, healthcare providers, and the healthcare industry as a whole.

58. Defendants owed a duty to Plaintiff and other healthcare providers, as well as the patients whose information Defendants stored, to protect sensitive and personally identifying information by complying with HIPAA and the FTCA, following FTC guidelines for cybersecurity, and adhering to industry standards for data protection.

59. Defendants breached the duty owed to Plaintiff and other healthcare providers by failing to comply with HIPAA and the FTCA, and failing to implement cybersecurity measures that were consistent with industry standards.

60. Defendants' failure to adhere to HIPAA, the FTCA, and industry standards enabled Blackcat to perpetrate the foreseeable and preventable Data Breach.

61. As a result of Defendants' failure to prevent the Data Breach through the implementation of adequate cybersecurity measures, Plaintiff and other medical practices have lost patients, incurred increased costs, and been unable to submit claims and receive payments for patient visits, prescriptions, and procedures, resulting in significant loss of revenue.

Class Action Allegations

62. Plaintiff seeks relief in its individual capacity and as a representative of all other similarly situated medical practices.

63. Plaintiff seeks certification of a Class defined as: all medical providers who utilized practice management and billing software that relied on the Change platform and who experienced an interruption in service and practice management capabilities as a result of the Data Breach.

64. Excluded from the defined Class are Defendants and their officers, directors, and employees, as well as any affiliate or legal representative of Defendants. Also excluded from the Class are any federal, state, or local government entities, any judicial officer presiding over this action, the staff of the judicial officer presiding over this action, the families of the aforementioned judicial officers and staff, and any juror assigned to this action.

65. **Numerosity**: The members of this Class are so numerous that individual joinder of all claims would be impracticable. There are hundreds of thousands of medical providers who utilized the Change network in their practice.

66. **Typicality**: Plaintiff's claims are typical of the members of the Class. Plaintiff's use of the Change network through the Aprima software and claims portals, as well as the service interruption they experienced, are emblematic of how Class members utilized the Change network and were impacted by the Data Breach. The duties owed by Defendants to Plaintiff are representative of the duties owed by Defendants to the Class at large.

67. **Adequacy**: Plaintiff is a member of the Class and will vigorously pursue all claims on behalf of the Class. Plaintiff has no conflicts of interest with the Class and Plaintiff's

claims are not subject to any unique individual defenses. Plaintiff has retained counsel who is experienced in class action and data breach litigation.

68. **Commonality**: There are questions of law and fact that are common to the Class and which predominate over the questions of law and fact that might arise in individual cases. These questions include, but are not limited to:

(a) The scope of the duty owed by Defendants to the Class to protect data and provide uninterrupted service;

(b) Whether Defendants' cyber security measures complied with the applicable regulatory framework including HIPAA, the FTCA, and industry standards for data protection;

(c) Whether Defendants' failure to protect the data stored on the Change network amounts to a breach of the duty owed to the Class;

(d) Whether Defendants' failure to implement adequate security measures amounts to a breach of the duty owed to the Class;

(e) Whether Defendants' failure to protect the data stored on the Change network proximately caused damages to the Class, as well as the nature and extent of those damages; and,

(f) Whether Defendants' failure to promptly restore service following the Data Breach was a breach of the duty owed to the Class.

69. **Superiority**: The purpose of this Class action is to permit litigation against Defendants even when damages to an individual member of the Class may not be sufficient to justify litigation. Individual litigation by each Class member would not be efficient or practicable and would raise the possibility of inconsistent and contradictory judgments. A class action is

superior to any other available means for the adjudication of these claims. Plaintiff is not aware of, and does not anticipate, any difficulties in the management of this Class litigation.

70. **Ascertainability**: The Class may be defined by objective criteria and the appropriate members of the Class can be readily ascertained.

COUNT I – NEGLIGENCE

On Behalf of Plaintiff and the Class v. Defendants

71. Plaintiff incorporates by reference the averments set forth in Paragraphs 1 through 70 as though the same were fully set forth herein.

72. Defendants collected, stored, and made commercial use of personal identifiers and other sensitive information relating to patients treated by or seeking treatment from Plaintiff and the members of the Class.

73. Defendants owed a duty to Plaintiff and the Class to protect the sensitive information stored on the Change platform from unauthorized access and disclosure and to maintain uninterrupted service through the Change platform.

74. Defendants' duty to Plaintiff and the Class to protect sensitive information from unauthorized access and disclosure arises from federal statutes and regulations, the common law, and industry standards for cyber security.

75. Defendants knew or should have known that the information they stored on the Change network was a priority target for cyber criminals and was vulnerable cyber attacks.

76. Defendants breached their duty owed to Plaintiff and the Class by:

(a) Failing to maintain an adequate date security system;

(b) Failing to protect patients' sensitive information;

(c) Failing to prevent the theft and possible dissemination of sensitive information;

(d) Failing to implement policies to restrict network and data access to properly authorized individuals;

(e) Failing to address credible security warnings and threats;

(f) Failing to maintain up-to-date security patches to remediate vulnerabilities;

(g) Failing to monitor the CIST website for information about current threats and associated patches;

(h) Failing to utilize adequate encryption for the storage and transmission of sensitive information;

(i) Failing to maintain audit logs and access reports to understand exactly how and by whom their network was being accessed;

(j) Failing to hire qualified cybersecurity experts to run the UHG audit committee and otherwise oversee and implement UHG's cybersecurity systems; and,

(k) Failing to train employees on basic cybersecurity principles.

77. As a result of Defendants' failure to protect the data stored on the Change network, Defendants' network security was breached and the Change platform that Plaintiff and the Class relied upon was taken offline for weeks or months depending on which specific platform the Class member used.

78. Defendants' breach of the duty owed to Plaintiff and the Class caused members of the Class to sustain damages such as:

(a) Missed payments for patient visits, prescriptions, and procedures;

(b) Inability to verify patient coverage prior to rendering treatment;

(c) Inability to calculate patient co-pays and deductibles;

(d) Inability to submit claims for processing and remittance;

(e) Increased operational expenses associated with hiring additional staff and engaging in the inefficient process of performing eligibility verifications and claim submissions manually;

(f) Inability to treat certain patients due to the unavailability of ERAs; and,

(g) Inability to receive payments for services rendered.

WHEREFORE, Plaintiff and the Class demand judgment in their favor and against Defendants and an award of damages to compensate them for damages sustained as a result of the Data Breach. Plaintiff and the Class also seek payment of costs and expenses as may be warranted.

COUNT II – NEGLIGENT UNDERTAKING

On Behalf of Plaintiff and the Class v. Defendants

79. Plaintiff incorporates by reference the averments set forth in Paragraphs 1 through 70 as though the same were fully set forth herein.

80. By owning and operating Change, a claims clearinghouse and data center, Defendants undertook to provide services for the benefit of Plaintiff and the Class.

81. In undertaking to provide services for the benefit of Plaintiff and the Class, Defendants knew or should have known of the necessity to heed credible security warnings and implement cybersecurity policies, practices, and protocols that were consistent with industry standards and the regulatory framework establish by HIPAA and the FTCA.

82. Only Defendants were in the position to ensure that their cybersecurity policies, practices, and protocols were consistent with industry standards and the regulatory framework established by HIPAA and the FTCA.

83. In undertaking to provide services for the benefit of Plaintiff and the Class, Defendants knew or should have known of the necessity to heed credible security warnings and implement cybersecurity policies, practices, and protocols that were sufficient to protect the sensitive data stored on their systems and networks.

84. Only Defendants were in the position to ensure that their cybersecurity policies, practices, and protocols were sufficient to protect the sensitive data stored on their systems and networks.

85. Plaintiff and the Class relied on Defendants to undertake their duty to provide services for the benefit of Plaintiff and the Class in a manner that protected the sensitive data stored on Defendants' systems and networks and that would avoid lengthy interruptions of service.

86. Defendants failed to abide by their duty owed to Plaintiff and the Class to heed credible security warnings and implement cybersecurity policies, practices, and protocols that were consistent with industry standards and the regulatory framework establish by HIPAA and the FTCA.

87. Defendants failed to provide services for the benefit of Plaintiff and the Class in a manner that protected the sensitive data stored on Defendants' systems and networks and that would avoid lengthy interruptions of service.

88. Defendants knew or should have known that their failure to implement cybersecurity policies, practices, and protocols that were consistent with industry standards and the regulatory framework establish by HIPAA and the FTCA increased the risk of harm to Plaintiff and the Class.

89. By undertaking to provide services for the benefit of Plaintiff and the Class, and by doing so without heeding credible security warnings and implementing cybersecurity policies, practices, and protocols that were consistent with industry standards and the regulatory framework establish by HIPAA and the FTCA, Defendants increased the risk of harm to Plaintiff and the Class beyond what it would have been had Defendants not undertaken to provide services for the benefit of Plaintiff and the Class.

90. Defendants' negligence in undertaking to provide services for the benefit of Plaintiff and the Class increased the risk of harm and did in fact cause harm to Plaintiff and the Class.

WHEREFORE, Plaintiff and the Class demand judgment in their favor and against Defendants and an award of damages to compensate them for damages sustained as a result of the Data Breach. Plaintiff and the Class also seek payment of costs and expenses as may be warranted.

COUNT III – UNJUST ENRICHMENT

On Behalf of Plaintiff and the Class v. Defendants

91. Plaintiff incorporates by reference the averments set forth in Paragraphs 1 through 70 as though the same were fully set forth herein.

92. By utilizing the claims processing and data storage services provided by Defendants, Plaintiff and the Class conferred a benefit on Defendants in the form of increased revenue.

93. Defendants failed to provide secure and uninterrupted claims processing and data storage services to Plaintiff and the Class.

94. Defendants retained the benefit conferred by Plaintiff and the Class.

95. Because Defendants failed to provide the secure and uninterrupted claims processing and data storage services that Plaintiff and the Class relied upon, which failure caused harm to Plaintiff and the Class, Defendants' retention of the benefit conferred on them by Plaintiff and the Class is unjust and inequitable.

96. Equity will be served by requiring Defendants to disgorge to Plaintiff and the Class the benefits conferred on them by Plaintiff and the Class.

WHEREFORE, Plaintiff and the Class demand judgment in their favor and against Defendants and an award of damages commensurate to the value of the benefit conferred on and unjustly retained by Defendants. Plaintiff and the Class also seek payment of costs and expenses as may be warranted.

COUNT VI – DECLARATORY JUDGMENT
On Behalf of Plaintiff and the Class v. Defendants

97. Plaintiff incorporates by reference the averments set forth in Paragraphs 1 through 70 as though the same were fully set forth herein.

98. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of statutes, rules, and regulations described herein.

99. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' past, ongoing, and prospective duties to implement adequate cybersecurity policies, practices, and protocols in the course of providing claims processing and data storage services to Plaintiff and the Class. There is an ongoing dispute as to whether Defendants' cybsecurity policies, practices, and protocols are compliant with HIPAA and the FTCA and sufficient to

reasonably ensure that Defendants will be able to render secure and uninterrupted services to Plaintiff and the Class.

100. Defendants still possess sensitive information that is crucial to the business operations of Plaintiff and the Class, and their failure to implement cyber security policies, practices, and protocols are compliant with HIPAA and the FTCA creates an ongoing increased risk of data breaches and interruptions in crucial services.

101. Pursuant to the Declaratory Judgment Act, Plaintiff and the Class seek a declaration that (1) Defendants' existing cyber security policies, practices, and protocols do not comply with their duty of care owed to Plaintiff and the Class; and (2) in order to comply with their duty of care Defendants must implement cybersecurity policies, practices, and protocols that are consistent with industry standards and compliant with HIPAA and the FTCA such as:

(a) encrypting all sensitive information that is stored or disseminated to third parties;

(b) maintaining up-to-date anti-malware programs on all computers and servers;

(c) checking websites of the Cybersecurity & Infrastructure Security Agency and software vendors for alerts as to new vulnerabilities and patches;

(d) restricting employees' ability to download unauthorized software;

(e) scanning computers to identify and close unnecessary network connections;

(f) adding additional layers of encryption to particularly sensitive information; and

(g) monitoring web applications which can be particularly susceptible to certain kinds of hacks.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff and the Class respectfully request the following relief:

(a) That the Court certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure and appoint Plaintiff as class representative and Plaintiff's counsel as Class Counsel;

(b) That the Court declare that Defendants' existing cybersecurity policies, practices, and protocols are not compliant with their duty of care owed to Plaintiff and the Class;

(c) That the Court award compensatory, consequential, and general damages to Plaintiff and the Class;

(d) That the Court award to Plaintiff and the Class the expenses, costs, and attorneys' fees incurred in this litigation; and

(e) That the Court award pre-judgment and post-judgment interest at the maximum legal rate along with any other relief and damages that it deems just and proper.

JURY TRIAL DEMANDED

Plaintiff and the Class demand a jury trial on all claims so triable.

Respectfully submitted,

Dated: June 24, 2024

By: /s/ David A. Goodwin
Daniel E. Gustafson (#202241)
David A. Goodwin (#0386715)
GUSTAFSON GLUEK PLLC
Canadian Pacific Plaza
120 South Sixth Street, Suite 2600
Minneapolis, MN 55402
Tel: (612) 333-8844
dgustafson@gustafsongluek.com
dgoodwin@gustafsongluek.com

Roberta Liebenberg*
Gerard A. Dever*
Mary L. Russell*
FINE, KAPLAN AND BLACK, RPC
One South Broad St., Suite 2300
Philadelphia, PA 19107
Tel: (215) 567-6565
rliebenberg@finekaplan.com
gdever@finekaplan.com
mrussell@finekaplan.com

Linda P. Nussbaum*
NUSSBAUM LAW GROUP, P.C.
1133 Avenue of the Americas, 31st Floor
New York, NY 10036
Tel: (917) 438-9102
lnussbaum@nussbaumpc.com

Jack Meyerson*
Matthew Miller*
MEYERSON & MILLER
1600 Market Street, Suite 1305
Philadelphia, PA 19103
Tel: (609) 703-0414
jmeyerson@meyersonlawfirm.com
mmiller@meyersonlawfirm.com

**To be admitted Pro Hac Vice*